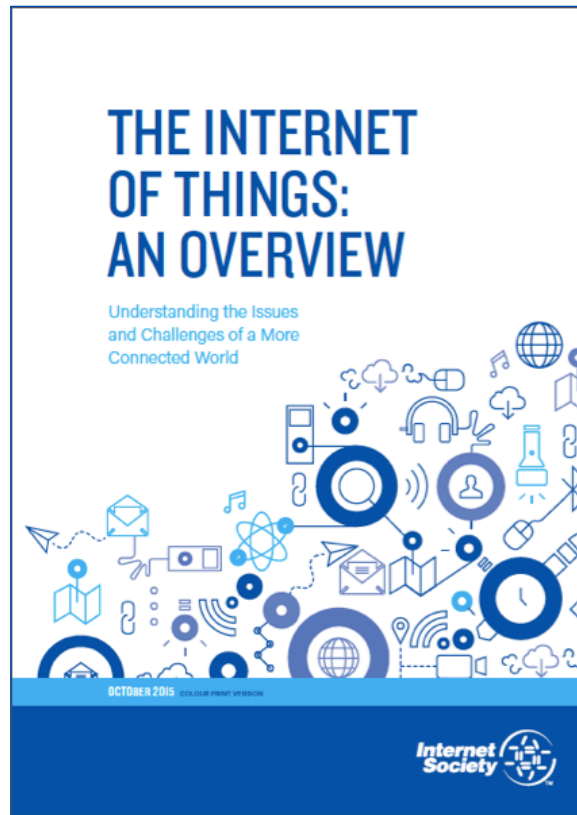# The Internet of Things: an overview

"Workshop on New Frontiers in Internet of Things"

Telecommunications/ICT4D Laboratory (T/ICT4D) of the Abdus Salam International Centre for Theoretical Physics (ICTP)

17 March 2016 (Trieste, Italy)

Internet Society

Setting the scene

THE INTERNET
OF THINGS:
AN OVERVIEW

Understanding the Issues
and Challenges of a More
Connected World

OCTOBER 2015 COLOUR PRINT VERSION

Internet
Society

- **About the Internet Society**

- **IoT Concepts & Drivers**

- **IoT Key Challenges**
  - **Security**
  - **Privacy**
  - **Interoperability**

About the
Internet Society

Who we are

➢ Global not-for-profit organization, founded in 1992

➢ Independent thought leader and advocate on issues impacting the Internet and its users

➢ Organizational home of the Internet Engineering Task Force (IETF)

Internet Society

Our Mission

To promote the open development, evolution, and use of the Internet for the benefit of all people throughout the world.

Internet Society™

Our Global Presence

Internet Society ™

NORTH AMERICA

EUROPE

THE MIDDLE EAST

AFRICA

ASIA

LATIN AMERICA/CARIBBEAN

116
Chapters
Worldwide

80,000+
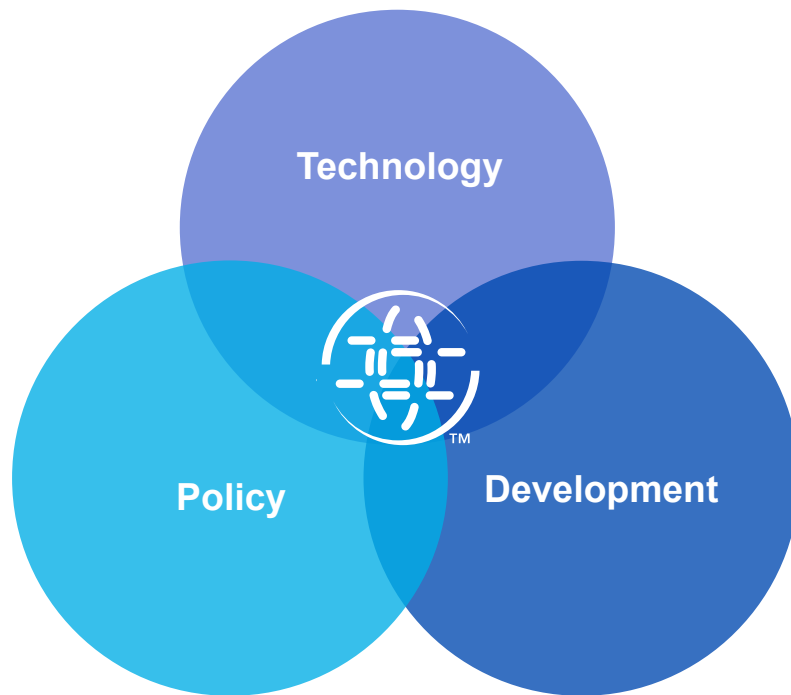Individual Members

143
Organization
Members

6
Regional
Bureaus

21
Countries with
ISOC Offices

How we work

We harness global expertise and work at the at the intersection of Internet:
- **policy**,
- **technology**, and
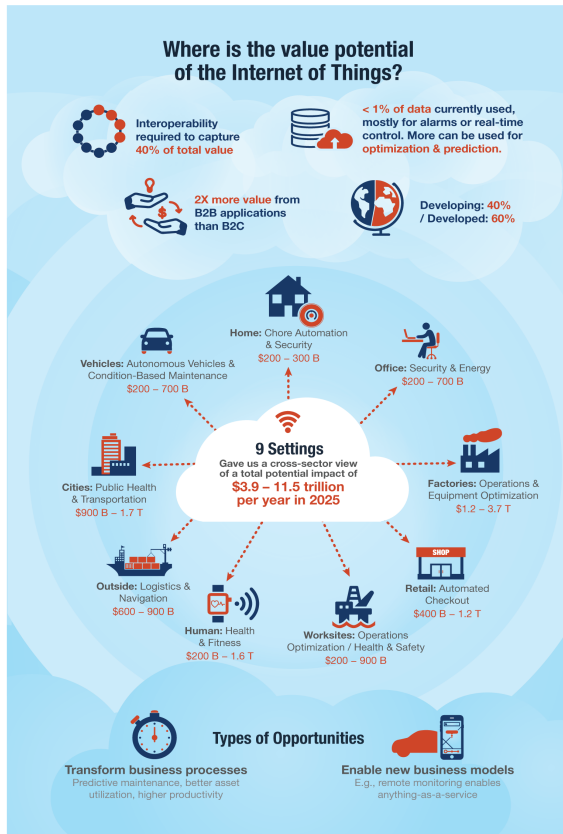- **development**

2016 Agenda Focus:

- **Promoting Trust in the Internet**
- **Connecting the Unconnected**

If you care about the Internet, join us!

IoT concepts and drivers

What is IoT?

- **Despite the buzz, no single definition**
  - Or agreed numbers, or categories, or taxonomies ...
  - Different emphasis on different aspects of the concept

- **Functionally:** The extension of network connectivity and computing capability to a variety of objects, devices, sensors and everyday items allowing them to generate/ exchange data, often with remote with data analytic/ management capabilities

- **As Value:** Data & what can be done with it

- **As a Vision:** The realization of a 'hyper-connected" world
  - This is why it matters
  - This is why it's hard

One view, from McKinsey Global Institute:

Where is the value potential of the Internet of Things?

Interoperability required to capture 40% of total value

< 1% of data currently used, mostly for alarms or real-time control. More can be used for optimization & prediction.

2X more value from B2B applications than B2C

Developing: 40% / Developed: 60%

9 Settings
Gave us a cross-sector view of a total potential impact of **$3.9 – 11.5 trillion per year in 2025**

Home: Chore Automation & Security $200 – 300 B

Vehicles: Autonomous Vehicles & Condition-Based Maintenance $200 – 700 B

Office: Security & Energy $200 – 700 B

Cities: Public Health & Transportation $900 B – 1.7 T

Factories: Operations & Equipment Optimization $1.2 – 3.7 T

Outside: Logistics & Navigation $600 – 900 B

Human: Health & Fitness $200 B – 1.6 T

Worksites: Operations Optimization / Health & Safety $200 – 900 B

Retail: Automated Checkout $400 B – 1.2 T

Types of Opportunities

Transform business processes Predictive maintenance, better asset utilization, higher productivity

Enable new business models E.g., remote monitoring enables anything-as-a-service

Computers & Networks & Things

"Machine to Machine" (M2M)
(~1970s +)

Internet of Things Beginnings

Carnegie Mellon Internet
Coke Machine (1982, 1990)

Internet Toaster
(1990)

Trojan Room
Coffee Pot
(first webcam)
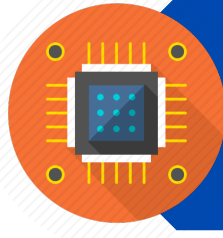(1991)

If it's not new, why now?:

A Confluence of Market Trends
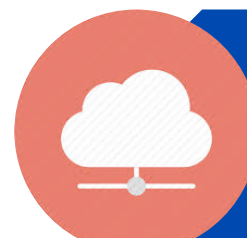
UBIQUITOUS CONNECTIVITY

COMPUTING ECONOMICS

ADVANCES IN DATA ANALYTICS

WIDESPREAD ADOPTION OF IP

MINIATURIZATION

RISE OF CLOUD COMPUTING

IoT Challenges

Key IoT Challenges

SECURITY

PRIVACY

INTEROPERABILITY AND STANDARDS

LEGAL, REGULATORY AND RIGHTS

EMERGING ECONOMIES AND DEVELOPMENT

Key IoT Challenges

🔒 **SECURITY**

👁 **PRIVACY**

⚙ **INTEROPERABILITY AND STANDARDS**

⚖ **LEGAL, REGULATORY AND RIGHTS**

🌐 **EMERGING ECONOMIES AND DEVELOPMENT**

Security

Security must be a fundamental priority

- Security is the most pressing and important IoT challenge for industry, users, and the Internet.

- Growth in devices increases the surface available for cyber attack

- Poorly secured devices affect the security of the Internet and other devices *globally*, not just *locally*.

Developers and users of IoT devices and systems have a collective obligation to ensure they do not expose others and the Internet itself to potential harm.

A spectrum of unique smart object security challenges

- Cost/Size/Functionality

- Volume of Identical Devices

- Deployment at Mass Scale

- Long Service Life

- No / Limited Upgradability

- Limited Visibility into Internal Workings

- Embedded Devices

- Physical Security Vulnerabilities

- Unintended Use & BYOIoT

See also IETF RFC 7452 *Architectural Considerations in Smart Object Networking*

Collaborative Security approach: developing solutions in the context of principles

|	
Fostering Confidence / Protecting Opportunities	_Opportunities_ for individuals, business, economy and and society will only be realized if there is _confidence_ in the Internet, systems, and technologies (including IoT).
Collective Responsibility	No security threats or solutions exist in isolation. Requires collective responsibility, a common understanding of problems, shared solutions, common benefits, and open communication channels.
Uphold Fundamental Properties and Values	Security solutions should be fully integrated with the important objectives of preserving the fundamental properties of the Internet and fundamental rights.
Evolution and Consensus	Security solutions need to be flexible enough to evolve over time & responsive to new challenges. Focus needed on defining agreed problems and finding solutions, including incremental ones.
Think Globally, Act Locally	Creating security and trust requires different players (within their respective roles / responsibilities) to take action and close to where the issues are occurring.

Privacy

IoT is evolving into an Internet of sensors and delving deeper into our personal lives

A couple of random anecdotes …

Fitbit readings reveal more than fitness
e.g. heartbreak and pregnancy

Eye-tracking software may reveal
early onset of alzheimers
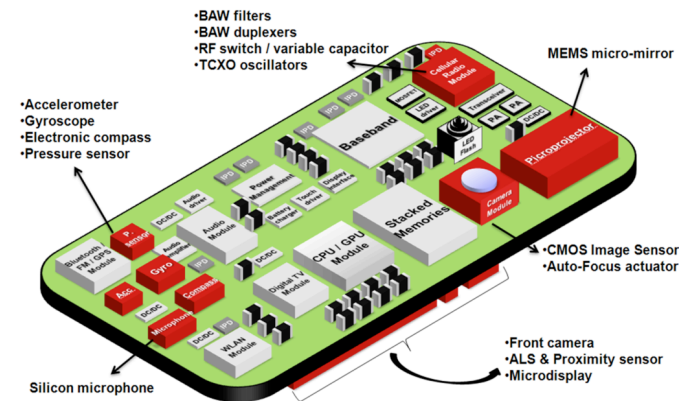
➢ *Mobile computing enabled sensors to travel with us*

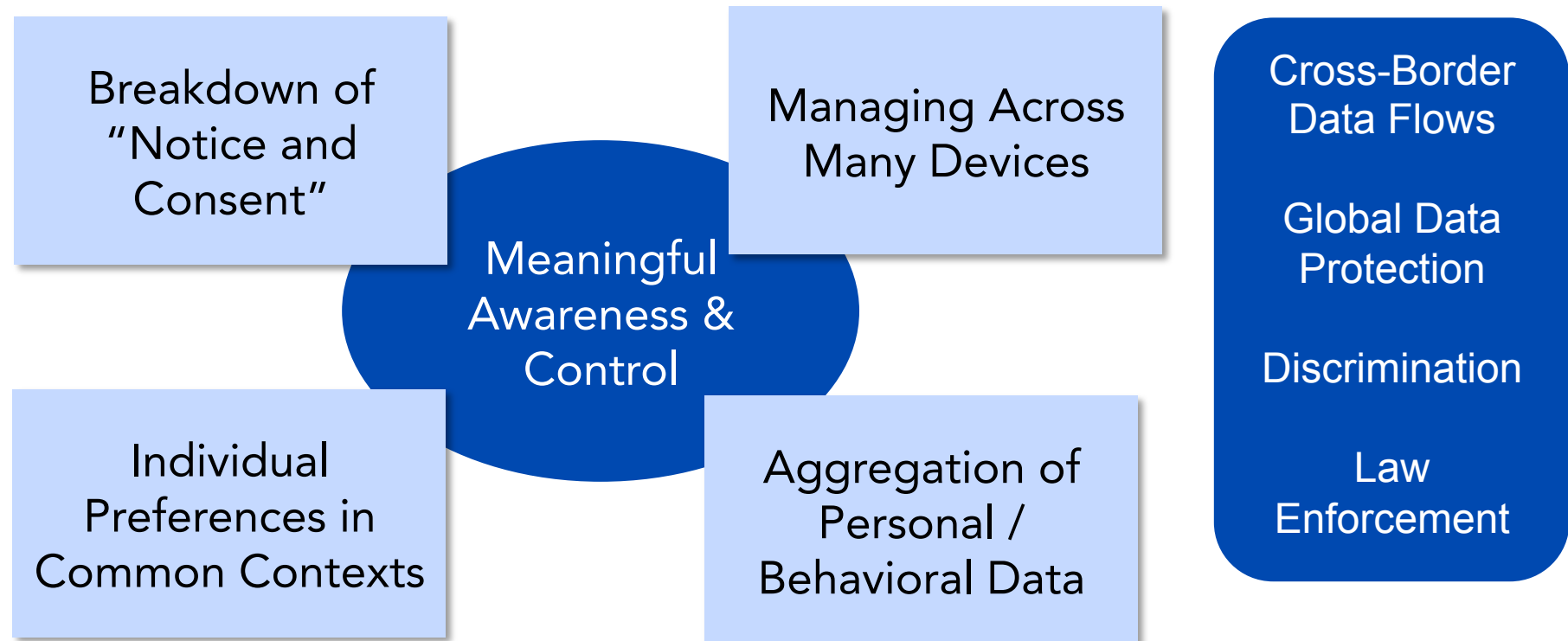➢ *IoT enables sensors to be all around us*

Privacy and IoT: data is a double-edged sword

- **Data streams /analytics that drive the value of IoT can also paint very detailed and intrusive pictures of our lives**

- **Expands the feasibility / reach of surveillance and tracking**

- **Redefining the debate about privacy issues**
  - Could dramatically change the ways personal data is collected, analyzed, used and protected
  - New privacy risks

- **Implications for our:**
  - Basic rights
  - Sense of personal safety and control
  - Ability to trust the Internet and devices connected to it

17 March 2016

Identifying the unique from the noise

Dimensions of privacy challenges in IoT

Breakdown of "Notice and Consent"

Individual Preferences in Common Contexts

Meaningful Awareness & Control

Managing Across Many Devices

Aggregation of Personal / Behavioral Data

Cross-Border Data Flows

Global Data Protection

Discrimination

Law Enforcement

Enhancing privacy in IoT

Strategies need to be developed that respect individual privacy choices across a broad spectrum of expectations, while still fostering innovation in new technology and services.

- Traditional online privacy models may not fit

Adapting/adopting basic privacy principles, such as:

- Transparency/Openness

- Meaningful Choice

- Data Minimization

- Use Limitation, etc.

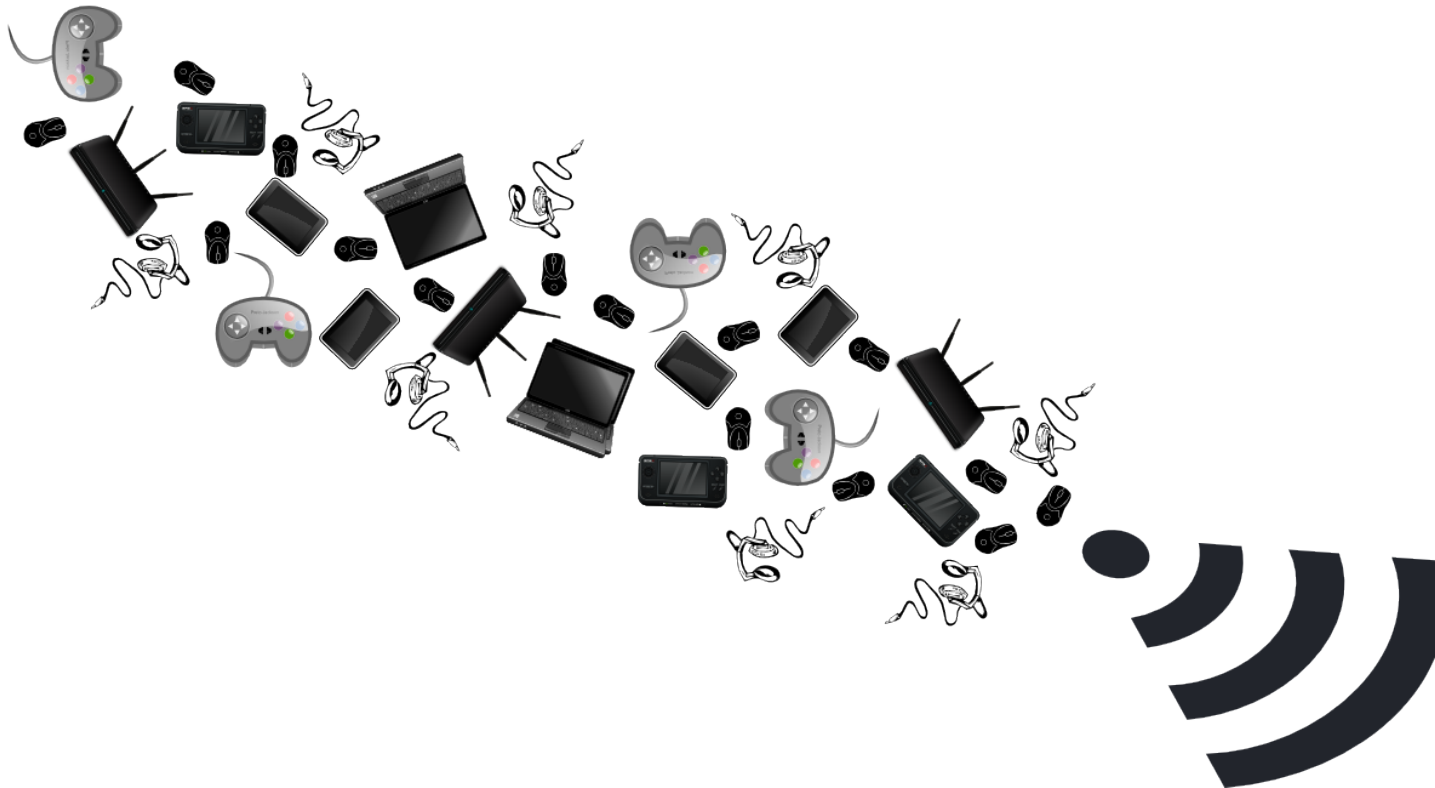# IoT identifiers and privacy – an example

Photo from Flickr Commons: jjfbbennett wifi bug modified aspect

Wi-Fi Internet connectivity and privacy

- Wi-Fi enabled devices have a Layer-2 address, known as a "MAC address"

- Most Wi-Fi enabled devices are assigned a globally unique address by the manufacturer

- These MAC addresses can be observed by anybody who can receive the signal transmitted by the network interface

- Wi-Fi enabled devices expose this address when actively scanning for an available wireless network

- This makes tracking a Wi-Fi enabled device (e.g. a smartphone) in time and space relatively easy

Monitoring Wi-Fi enabled devices

Remember the short-lived London "smart" recycling bins that logged the MAC addresses of passersby's Wi-Fi enabled devices (smartphones, tablets, etc.)

The first month of operation, the bins collected > 1,000,000 unique MAC addresses => > 1,000,000 unique devices

A week's data
for one bin
over time

Reference: http://qz.com/112873/this-recycling-bin-is-following-you/
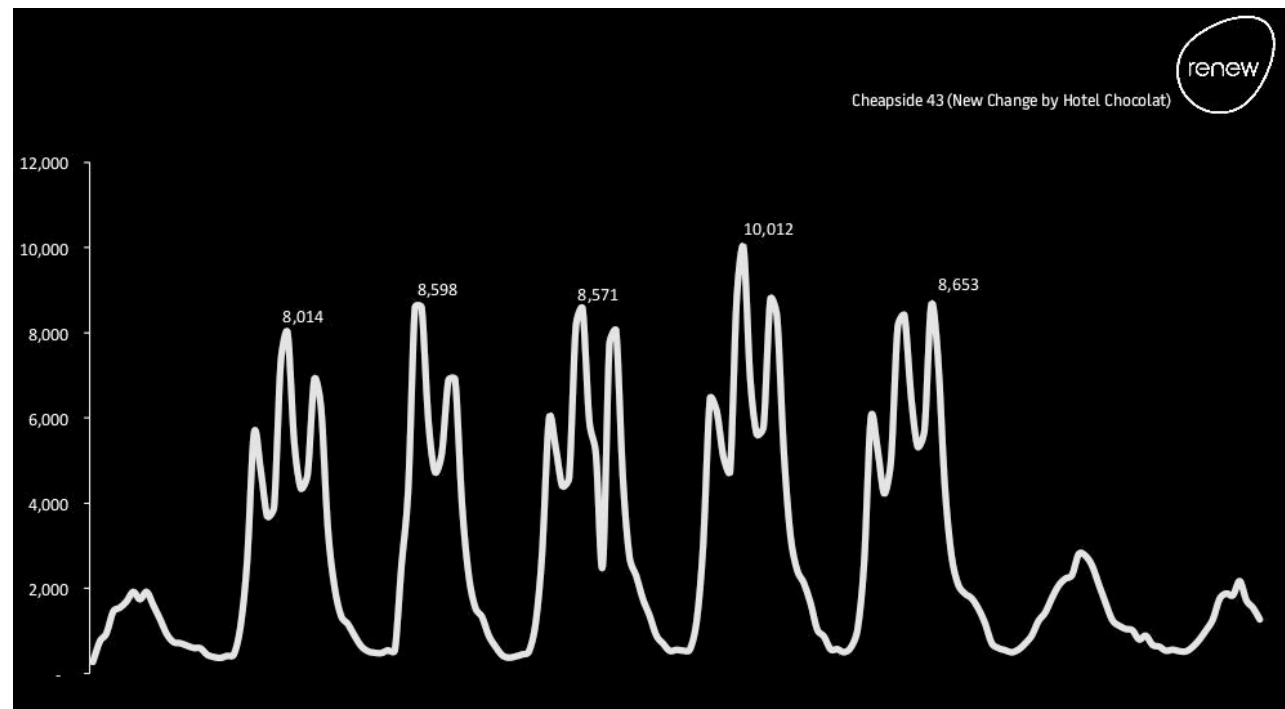
Mitigating this privacy threat

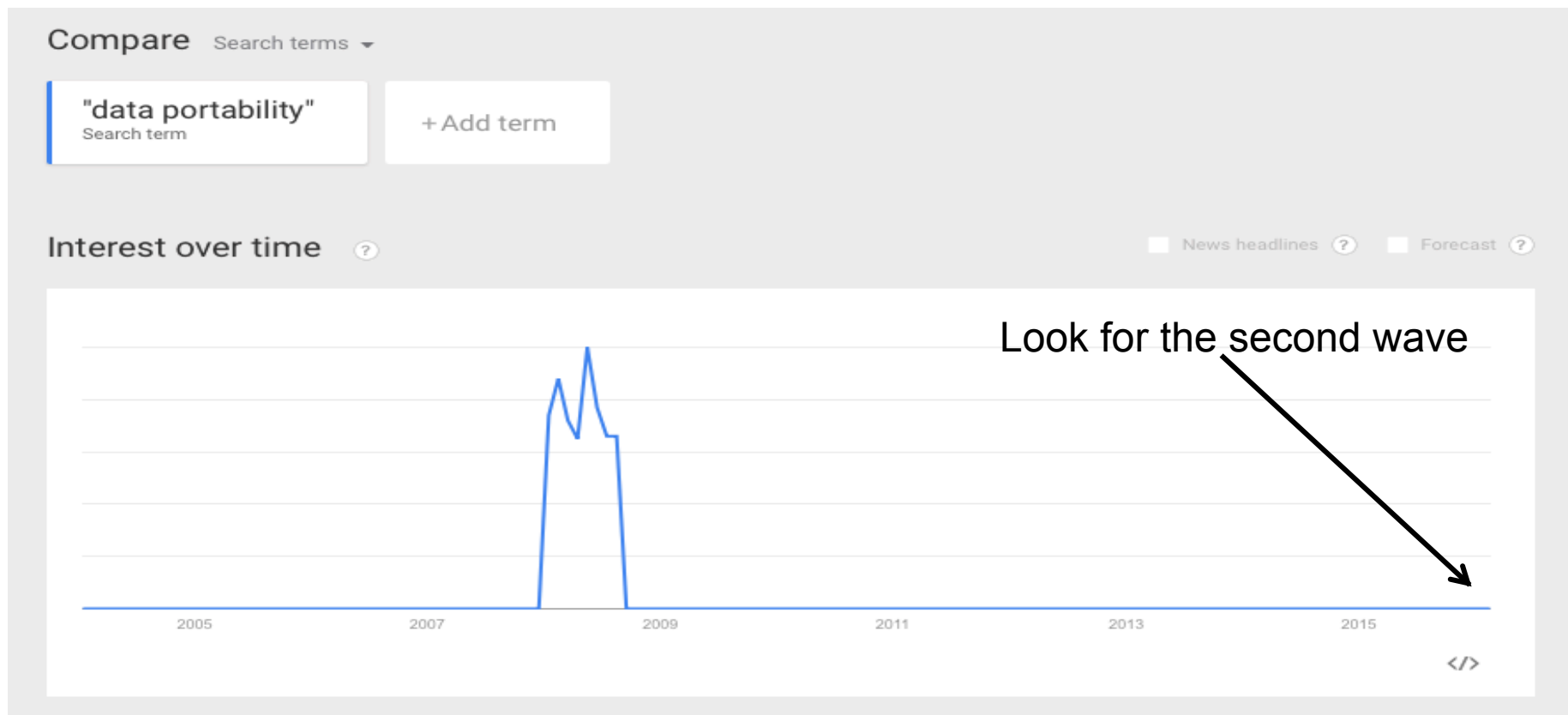IEEE 802 EC Privacy Recommendation Study Group created

Wi-Fi enabled device MAC address randomisation experiments at IETF and IEEE 802 meetings – a joint IEEE/IETF project

Some issues to consider:

- What is the impact? (on the operation of other Internet protocols, provision of services, on the user experience, etc.)

- What randomisation polices work in what contexts? (e.g. enterprise network, public Wi-Fi hotspot)

- Potential address collisions

- Is the randomisation random enough?

read more: https://www.internetsociety.org/publications/ietf-journal-march-2015/wifi-privacy-trials-ietf-91-and-ietf-92
http://www.it.uc3m.es/cjbc/papers/pdf/2015_bernardos_cscn_privacy.pdf
http://www.ieee802.org/PrivRecsg/

What problem was the first wave of data portability trying to solve?

the ability to switch services (and avoid vendor lock-in)

encourage interoperability, and open standards

* Arguably grounded more in consumer protection than privacy

Some challenges:

➢ proprietary data formats

➢ the network effect as an impediment to switching even with the availability of data portability

What has happened while IoT was emerging?

The emergence of data portability as part of the service

Some "teething issues" (between competitors)

⇒ limits and conditions, such as:

      partial export (e.g. excluding contacts information)

      only with some providers

      only for less core services

      download only, no automatic import via API

How data portability evolves could have a significant impact for IoT

Data portability is emerging in legal frameworks

There is an emerging appetite for creating a legal entitlement or recognising a right to data portability (e.g. Article 18 of the *EU General Data Protection Regulation*)

Data portability has its origins in privacy/data protection doctrine, which influences its reach and application

Image from Flickr Commons – uploaded by Sean MacEntee

Interoperability & Standards

I&S: Not just a tech challenge, it's a market issue

40% Interoperability is necessary to create up to 40 percent of the economic value generated by IoT
-- McKinsey Global Institute

Efficiency
Scale
Market Value

Q: What are the greatest barriers inhibiting business from adopting the industrial Internet?

Source: World Economic Forum

Lack of interoperability or standards
- Overall — 65%
- N. America — 60%
- Europe — 67%

Security concerns
- Overall — 64%
- N. America — 72%
- Europe — 60%

Legend:
- Overall
- N. America
- Europe

Interoperability / Standards Considerations

- **Complex / Dynamic Service Delivery Chains and Use Cases**

- **Land Rush and Schedule Risk**

- **Proliferation of Standards Efforts?**

Can overlapping efforts be avoided without undue coordination overhead?

- **Where is Interoperability needed?**

- **Reusable building blocks**

- **Best Practices and Reference Models**
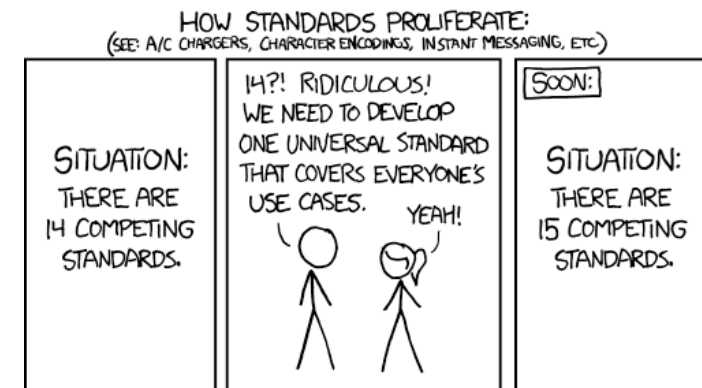
Ultimately, its about advancing innovation and user choice

Closing thoughts

- **IoT is happening now, with tremendous transformational potential**

- **But the challenges must be addressed to realise the opportunities and benefits**

    - **Significant. Real. But, not insurmountable**

    - **Solutions won't be found by simply pitting promise vs. peril**

- **It will take informed engagement, dialogue, and collaboration across a range of stakeholders to find solutions and to plot the most effective ways forward.**

Thank you

17 March 2016

The Internet of Things: An Overview
Understanding the Issues and Challenges of More Connected World

http://www.internetsociety.org/IoT

Christine Runnegar (runnegar@isoc.org)

THE INTERNET OF THINGS: AN OVERVIEW

Understanding the Issues and Challenges of a More Connected World

OCTOBER 2015

Internet Society

Internet Society